

Entorno Tecnológico. La revolución cuántica y la nueva computación

Fuente: La Jornada

CUAUHTEMOC VALDIOSERA R.

En un futuro más cercano de lo que pensamos, la información no tendrá que recorrer distancia alguna para llegar del emisor al receptor, porque las computadoras se basarán en la mecánica cuántica, que describe aquellos estados de la materia en los que las partículas se comportan como si no existiera el espacio.

Estamos ante otra de esas revoluciones interdisciplinarias que producen nuevas relaciones entre campos inicialmente casi inconexos. La teoría cuántica está alcanzando también a la información, no sólo en sus métodos de procesado, sino entrando en su propia concepción. La posibilidad de construir computadoras cuánticas permitirá estudiar novedosas formas de tratar la información hasta ahora insospechadas, además de poner de manifiesto ciertos comportamientos cuánticos fundamentales, de momento sólo plasmados como experimentos mentales en los libros de texto.

El ingenio de los investigadores y los recursos económicos puestos en juego nos inducen a pensar que en 20 o 30 años se pueda disponer de un prototipo de una computadora cuántica que permita realizar alguna tarea de interés. Si la situación actual es análoga a la que existía en los años 40, cuando se construyó la primera computadora, el futuro cercano nos depara todavía muchas sorpresas.

La computadora ha acompañado al hombre a lo largo de la historia. Las máquinas de cálculo se han ido complicando a la vez que se hacían más versátiles, desde el ábaco chino desarrollado hace milenios, pasando por las calculadoras de Pascal, hasta llegar al primer ordenador, el Electronic Numerical Integrator and Computer o ENIAC, construido en la Universidad de Pensilvania para los Ballistic Research Laboratories, hacia 1946. El ENIAC constaba de 17 mil 468 tubos de vacío, pesaba 27 mil kilos, ocupaba toda una habitación de 460 m³ y realizaba 5 mil operaciones por segundo. A medida que las computadoras aumentan su velocidad de funcionamiento, su tamaño disminuye. La miniaturización ha llevado de los relés, válvulas y transistores hasta los actuales circuitos integrados, pero, ¿dónde está el límite? Según la primera ley de Moore, "el número de transistores que se pueden introducir en un chip se incrementa de forma exponencial (cada 3.4 años, este número se multiplica por cuatro)". Parece que el próximo nivel será el molecular. A este nivel no sólo hay que tener en cuenta la mecánica cuántica para conseguir que los dispositivos funcionen correctamente, sino que la mecánica cuántica participa activamente en el comportamiento global.

Hacia el inicio de la década de los 60, Rolf Landauer comenzó a preguntarse si las leyes físicas imponían limitaciones al proceso de cómputo. En concreto se preguntaba sobre el origen del calor disipado por los procesadores, y si este calor era algo inherente a las leyes de la física o se debía a la falta de eficiencia de la tecnología disponible. La pregunta era: ¿será posible idear una puerta que funcione de forma reversible, y que por tanto no disipe energía? La teoría clásica de la computación no hacía referencia a la física del dispositivo. Se suponía que los fundamentos de tal teoría eran independientes de la realización física de los mismos. Hubieron de pasar 20 años hasta que Deutsch, Feynman y otros pusieran de manifiesto que esta idea es falsa, mostrando la conexión entre las leyes de la física y la información, y en concreto con la computación. A partir de aquí se produjo una de tantas uniones entre ideas distintas que han aparecido en la física: computación y mecánica cuántica. La computación cuántica surgió de esta unión.

La posibilidad de que una máquina de Turing cuántica pudiera hacer algo genuinamente cuántico fue propuesta por Richard Feynman en 1982. Mostró que ninguna máquina de Turing clásica podía simular algunos comportamientos cuánticos sin incurrir en una ralentización exponencial. Sin embargo, una máquina de Turing cuántica sí podía hacer una simulación efectiva. Feynman describió un "simulador cuántico universal" que simulaba el comportamiento de cualquier sistema físico finito. Desafortunadamente, Feynman no diseñó este simulador y su idea tuvo un poco de impacto en su época.

El siguiente paso se dio en 1985, cuando David Deutsch describió la primera máquina de Turing cuántica que establecía la posibilidad de construir un ordenador universal que puede programarse para simular cualquier sistema físico finito operando con unos recursos limitados.

Estas máquinas cuánticas usan una representación de la información algo distinta de la clásica. El fragmento de información clásica fundamental es el bit, entendiéndose como tal un sistema material que puede adoptar uno de los dos posibles estados distintos que representan dos valores lógicos (0 y 1 o sí y no, verdadero y falso, etcétera).

Si la codificación de la información es cuántica, y se hace a través de dos estados de un sistema microscópico, que por analogía al caso clásico podemos representar por los kets cuánticos $|0\rangle$ y $|1\rangle$, ahora también es posible un estado del sistema que sea una superposición coherente del tipo $Q = a|0\rangle + b|1\rangle$, denominado quantum-bit o qubit. Un átomo en una de tales superposiciones estaría en "ambos estados a la vez", no siendo ni un 0 ni un 1 clásicos. La existencia de estos estados "esquizofrénicos" nos indica que el computador cuántico tiene que poder tratarlos: generarlos y trabajar con ellos. Notemos que debido a que no existen restricciones acerca de los posibles valores de estos coeficientes a y b (salvo quizás la condición de normalización), en un solo qubit podríamos codificar una cantidad de información "infinita".

Dado que el tratamiento de la información cuántica es notablemente distinto del de la clásica, necesitamos algunas herramientas para construir los programas cuánticos. Se necesitan tres ingredientes básicos en el software cuántico. En primer lugar un conjunto apropiado de puertas.

Una forma de obtener puertas cuánticas es la cuantización de las puertas clásicas, que pasa por reinterpretar los bits como qubits. El propósito de los hilos es transmitir estados cuánticos de una a otra puerta y su forma concreta dependerá de las realizaciones tecnológicas concretas de los qubits.

Se puede demostrar que el conjunto de puertas cuánticas que afectan a un solo qubit, conjuntamente con las puertas llamadas control-not (que afectan a dos qubits), forman un conjunto universal con las que se puede construir cualquier programa cuántico.

El segundo ingrediente para el software cuántico son los algoritmos. A pesar del esfuerzo que se ha dedicado a la obtención de algoritmos que aprovechen el comportamiento cuántico, en la actualidad, su número es reducido.

Uno de los desafíos actuales más importantes es la construcción de un hardware cuántico apropiado, siendo el cuello de botella de los computadores cuánticos. Debido a los problemas de la creación, control y corrección de errores en las superposiciones coherentes de estados cuánticos, la tecnología actual que implementa puertas y circuitos cuánticos está en su infancia.

A pesar de todo se han construido puertas experimentales control-not de dos qubits, y se han usado algunas técnicas simples de corrección de errores. Para construir una computadora cuántica se necesitan resolver varios problemas: elección de los sistemas físicos que representan los qubits, control de las puertas cuánticas, control de los errores y posibilidad de escalar la computadora para tratar problemas de distinto tamaño. Con estos requerimientos se están estudiando diferentes sistemas físicos que se pueden clasificar dependiendo de sus características o de su interacción.

Existen otros comportamientos que están directamente relacionados con el tratamiento cuántico de la información, y con las computadoras cuánticas, concretamente la teleportación y los códigos densos. Para conseguir una teleportación completa es necesario realizar una medida que distinga entre los cuatro estados de Bell de dos partículas.

La primera realización práctica de la teleportación la llevó a cabo el grupo de Anton Zeilinger en 1997 (Universidad de Innsbruck), consiguiendo la teleportación del estado de polarización de un fotón a lo largo de un metro de distancia.

En 1998, en Los Alamos, se consiguió una teleportación intramolecular completa. Se teleportó un estado de spin nuclear de un carbono (Carbono-13 más alejado) al hidrógeno del tricloroetileno, usando técnicas RMN. También en la Universidad de Maryland (en 2000) se realizó la teleportación del estado de polarización de un fotón, realizando una medida de Bell completa.

Todas estas técnicas sólo usan estados de unas pocas partículas. En septiembre de 2001 (en la Universidad de Aarhus, Dinamarca) se consiguió el "entanglement" entre los spines totales de dos nubes que contienen trillones de átomos de cesio. A pesar de la corta vida de este estado, el experimento demostró que es posible crear estos estados en sistemas macroscópicos. Pero la teleportación al estilo Star Trek está aún lejos, pero estamos en el camino.

El autor agradece la información proporcionada por la Universidad Politécnica de Madrid